PingAccess®

Version 3.0

Getting Started

Copyright

© 2005-2014 Ping Identity® Corporation. All rights reserved.

PingAccess

Version 3.0
July, 2014

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Trademark

Ping Identity, the Ping Identity logo, PingAccess, PingFederate, and PingOne are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to the online documentation at *documentation.pingidentity.com* for the most current information.

From the web site, you may also download and refresh this PDF if it has been updated, as indicated by a change on this date: **July, 2014**.

Getting Started

Getting Started

This Getting Started guide will help you install PingAccess and start using it quickly. There are two ways to use PingAccess to protect your web applications - gateway and agent. The way you choose depends on your network design and security requirements. A single PingAccess Server can protect many web applications using a combination of both techniques. See the Deployment Guide for a detailed discussion of deployment options and Configuration by Use Case in this section for configuration instructions.

> To automatically configure PingAccess and PingFederate for demonstrating its base functionality, use the PingAccess Quickstart Demo App available for download from the Ping Identity Support & Downloads page.

To get started with PingAccess:

1. Install the Oracle JDK if it isn't installed already.
2. Install and start PingAccess on either Windows, Linux, or Mac.
3. Optional. Configuration Properties in the `run.properties` file.
4. Configure settings within PingAccess. What items you configure depends on your deployment plans.

> For help in successfully configuring PingAccess to meet your use case, see Configuration by Use Case.

System Requirements

System Requirements

PingAccess is certified as compatible for deployment and configuration with the minimum system specifications defined below.

Supported Platforms

- Windows Server 2008 R2 SP1
- Windows Server 2012 Standard
- Windows Server 2012 R2 Standard
- Red Hat Enterprise Linux ES 5.10
- Red Hat Enterprise Linux ES 6.5
- SUSE Linux Enterprise 11 SP3

Java Runtime Environment

- Oracle Java 7 update 60 (64-bit)
- Oracle Java 8 update 5 (64-bit)

Supported PingFederate

- PingFederate 7.2

Minimum Hardware Requirements

> Although it is possible to run PingAccess on less powerful hardware, the following guidelines accommodate disk space for default logging and auditing profiles and CPU resources for a moderate level of concurrent request processing.

- 4 CPU/Cores
- 2 GB of RAM
- 2.1 GB of available hard drive space

Minimum Hardware Recommendations

- Multi-CPU/Cores (8 or more)
- 4 GB of RAM
- 2.1 GB of available hard drive space

Supported Browsers for End Users

- Chrome
- Firefox
- Safari
- Internet Explorer (version 8 and higher)
- Android 4.0
- iOS 7

Supported Browsers for Admin Console

- Chrome
- Firefox
- Internet Explorer (version 9 and higher)

Audit Event Storage (External Database)

- Oracle 11g R2

Install the Oracle JDK

Install the Oracle JDK

The 64-bit version of JDK 7 (update 60 or higher) or JDK 8 (update 5 or higher) provides the supported environment for PingAccess.

You must install the Oracle JDK before installing PingAccess.

To install the Oracle JDK for Windows and Linux:

1. Download and install Oracle JDK from http://www.oracle.com/technetwork/java/javase/downloads/index.html.
2. Set the `JAVA_HOME` environment variable to the JDK installation directory path. Set the variable at either the system or user level.
3. Add the JDK `/bin` directory path to the `PATH` variable for your platform so it is available for scripts that depend on it.

Install PingAccess

Install PingAccess

Install PingAccess by extracting the downloaded distribution ZIP file.

On Linux we recommend that you install and run PingAccess under a local user (non-root) account.

To install PingAccess:

1. Ensure you are logged on to your system with appropriate privileges to install and run an application.
2. Verify that the JDK is installed and that environment and PATH variables are set correctly (see Install the Oracle JDK).
3. Extract the distribution ZIP file into an installation directory.
4. Request a license key via the Ping Identity licensing Web page (www.pingidentity.com/support-and-downloads/licensing.cfm).
5. Save the license key file in the directory `<pa_install>/conf` with the name `pingaccess.lic`.

PingAccess will not start without a valid license key file.

If you are deploying PingAccess in a cluster configuration, see Configure PingAccess Servers into a Cluster.

Uninstall PingAccess

1. Make sure that PingAccess is not running (see Start and Stop PingAccess).
2. Delete the PingAccess installation directory.

Running PingAccess as a Windows Service

Running PingAccess as a Windows Service

You can set up PingAccess to run in the background as a service on Windows running 64-bit processors.

Before performing this procedure, ensure that PingAccess runs normally by manually starting the server (see Run PingAccess for the First Time).

This installation enables PingAccess to start automatically when Windows is started or rebooted.

To run PingAccess as a Windows service:

1. Complete the steps above to install PingAccess.

   Ensure JAVA_HOME is set as a system variable (see Install the Oracle JDK).

2. Ensure you are logged on with full Administrator privileges.
3. Start PowerShell or Command Prompt as an Administrator.
4. In PowerShell or Command Prompt, run the install-service.bat file located in <pa_install>\sbin\windows.
5. Access the Windows **Control Panel** | **Administrative Tools** | **Services**.
6. Right-click **PingAccess Service** from the list of available services and select **Start**.
   The service starts immediately and restarts automatically on reboot. (You can change the default **Start type** setting in the **Properties** dialog.)

Running PingAccess as a Linux Service

Running PingAccess as a Linux Service

You can set up PingAccess to run in the background as a service on Linux. This enables PingAccess to start automatically when Linux is started or rebooted. The service will run as `root` user by default, or a specific user if specified.

Before performing this procedure, ensure that PingAccess runs normally by manually starting the server (see Run PingAccess for the First Time).

To set up PingAccess as a Linux service do the following steps:

1. Copy the PingAccess script file from `<PA_HOME>/sbin/linux/pingaccess` to `/etc/init.d`.
2. (Optional) Create a new user to run PingAccess.
3. Create the folder `/var/run/pingaccess` and ensure that the user who will run the service has read and write permission to the folder.
4. Edit the script file `/etc/init.d/pingaccess` and set the values of following variables at the beginning of the script:
   - `export JAVA_HOME=` specify the Java install folder
   - `export PA_HOME=` specify the PingAccess install folder
   - `export USER=` (optional) specify user name to run the service, or leave empty for default
5. Register the service by running the command "`chkconfig --add pingaccess`" from the `/etc/init.d` folder.
6. Make the service script executable by running the command "`chmod +x pingaccess`"

> ⚠ The service script will only start if JAVA_HOME and PA_HOME are set and the PingAccess license file is found.

Once registered, you can use the `service` command to control the pingaccess service. The available commands are:

- start
- stop
- restart
- status - shows the status of the PingAccess service and the PID

For example, run the command "`service pingaccess restart`" to stop and restart PingAccess.

Run PingAccess for the First Time

Run PingAccess for the First Time

1. Start PingAccess by running the following script:
   (Windows) <pa_install>\bin\run.bat
   (Linux) <pa_install>\bin\run.sh

   > ℹ The run.sh script requires bc, the GNU command line calculator. To install bc on SUSE, execute the following command: zypper install bc.

   Wait for the script to finish the startup---The server is started when you see the message “PingAccess running...” in the command window.

   > ℹ If you are using the PingAccess Quick-Start Application, at this point there are initialization steps for completing your setup. See the Quick-Start Application's ReadMeFirst for more information.

   > ℹ If you have not yet installed a PingAccess license, the server does not start up (see Install PingAccess for information on obtaining a license).

2. Launch your browser and go to:
   https://<DNS_NAME>:9000
   where <DNS_NAME> is the fully-qualified name of the machine running PingAccess.
3. Log on with the default username and password supplied with the distribution.
   Username: Administrator
   Password: 2Access
4. Read and accept the license agreement.
5. Change the default administrator password on the **First Time Login** screen and click **Continue**.

   > ℹ The new password must conform to the rules specified by the `pa.admin.user.password.regex` property in `run.properties`.

   The PingAccess administrative console appears.

Start and Stop PingAccess

Start and Stop PingAccess

Linux

To start PingAccess:

1. From a command prompt, change directories to <pa_install>\bin.
2. Execute the run.sh shell script.
   Wait for the script to execute. The server is started when you see the message “PingAccess running...” in the command window.

To stop PingAccess:
Enter Ctrl+C in the terminal window.

Windows

To start PingAccess:

1. From the **Start** > **Run** dialog or a command prompt, run the batch file:
   <pa_install>\bin\run.bat
   Or:
   Open the bin folder within your PingAccess installation and double-click the run.bat file.
2. Wait for the script to execute.
   The server is started when you see the message “PingAccess running...” in the command window.

To stop PingAccess:

1. Enter Ctrl+C in the command-prompt window.
2. Enter y to terminate the batch script when prompted.

All Platforms

To access the PingAccess administrative console:

1. Launch a Web browser window
2. Go to location `https://<DNS_NAME>:<PORT>` where `<DNS_NAME>` is the fully-qualified name of the machine running the PingAccess server and `<PORT>` is the port where the administrative console listens (default 9000). For example, `https://localhost:9000`.

Configuration by Use Case

Configuration by Use Case

Your next configuration steps depend on what type of deployment you are implementing. See the Deployment Guide for a detailed discussion of deployment considerations and best practices in designing your architecture. The following sections describe the configuration steps for the most common use cases:

- API Access Management Gateway Deployment
- Web Access Management Agent Deployment
- Web Access Management Gateway Deployment
- Auditing and Proxying Gateway Deployment

Next Steps

Once you complete the above configuration settings, your next steps are similar for all use cases:

- Configure Sites and Agents to define the target applications to be protected. Sites may need Site Authenticators to define the credentials the site expects for access control.
- Configure Applications and Resources to define the assets you wish to allow clients to access.
- Create Policies for the defined applications and resources to protect them.

API Access Management Gateway Deployment

API Access Management Gateway Deployment

The following section describes the important configuration options for deploying an API Gateway. See Deploying for Gateway API Access Management in the Deployment Guide for specific use case information.

Step	Description
Configure the connection to the PingFederate OAuth Authorization Server.	PingAccess uses this connection and credentials to validate incoming Access Tokens for securing API calls.
Configure the Resource Server OAuth Client.	The client must be registered with PingFederate and the client credentials configured in PingAccess to authenticate PingAccess when validating incoming Access Tokens.
Generate or Import Key Pairs and configure HTTP Listeners.	Defines the certificates and keys used to secure access to the PingAccess administrative console and secure incoming HTTPS requests at runtime.

Set up your cluster for high availability.	Facilitates high availability of critical services, and increases performance and overall system throughput.
Add trusted CA certificates.	Defines trust to certificates presented during outbound secure HTTPS connections.
Create a trusted certificate group.	Provides a trusted set of anchor certificates for use when authenticating outbound secure HTTPS connections.
Define virtual servers for protected applications.	Allows one server to share PingAccess Resources without requiring all Sites on the server to use the same host name. If SNI is available (Java 8), specific key pairs can be assigned to virtual hosts

Web Access Management Gateway Deployment

Web Access Management Gateway Deployment

The following section describes the important configuration options for a Web Access Management Gateway deployment. See Deploying for Gateway Web Access Management in the Deployment Guide for specific use case information.

Step	Description
Configure the connection to the PingFederate.	PingAccess uses PingFederate to manage web session and authentication.
Configure the OpenID Connect Relying Party Client for PingAccess.	The client must be registered with PingFederate and the client credentials configured in PingAccess to identify PingAccess when requesting authentication for users trying to access Web applications.
Configure Web session details to enable protection of Web Resources.	Configures settings for secure Web sessions such as timeout values, cookie parameters, and cryptographic algorithms.
Generate or Import Key Pairs and configure HTTP Listeners.	Defines the certificates and keys used to secure access to the PingAccess administrative console and secure incoming HTTPS requests at runtime.
Set up your cluster for high availability.	Facilitates high availability of critical services, and increases performance and overall system throughput.
Add trusted CA certificates.	Defines trust to certificates presented during outbound secure HTTPS connections.
Create a trusted certificate group.	Provides a trusted set of anchor certificates for use when authenticating outbound secure HTTPS connections.
Define virtual servers for protected Resources.	Allows one server to share PingAccess Resources without requiring all Sites on the server to use the same host name. If SNI is available (Java 8), specific key pairs can be assigned to virtual hosts.

Web Access Management Agent Deployment

Web Access Management Agent Deployment

The following section describes the important configuration options for a Web Access Management Agent deployment See Deploying for Agent Web Access Management for specific use case information.

First, PingAccess Agent needs to be deployed using the following steps:

1. Install PA Agent on Web Server - following instruction in PingAccess Agent for Apache Installation or PingAccess Agent for IIS Installation depending on your specific Web server.
2. Define the Agents and download agent bootstrap.properties file via the download field in the Shared Secrets field.
3. Deploy the agent bootstrap.properties file to agents following instructions in PingAccess Agent Configuration .

The rest of PingAccess deployment is similar to Web Access Management Gateway Deployment.

Step	Description
Configure the connection to the PingFederate.	PingAccess uses PingFederate to manage web session and authentication.
Configure the OpenID Connect Relying Party Client for PingAccess.	The client must be registered with PingFederate and the client credentials configured in PingAccess to identify PingAccess when requesting authentication for users trying to access Web applications.

Configure Web session details to enable protection of Web Resources.	Configures settings for secure Web sessions such as timeout values, cookie parameters, and cryptographic algorithms.
Generate or Import Key Pairs and configure HTTP Listeners.	Defines the certificates and keys used to secure access to the PingAccess administrative console and secure incoming HTTPS requests at runtime.
Set up your cluster for high availability.	Facilitates high availability of critical services, and increases performance and overall system throughput.
Add trusted CA certificates.	Defines trust to certificates presented during outbound secure HTTPS connections.
Create a trusted certificate group.	Provides a trusted set of anchor certificates for use when authenticating outbound secure HTTPS connections.
Define virtual servers for protected Resources.	Allows one server to share PingAccess Resources without requiring all Sites on the server to use the same host name. If SNI is available (Java 8), specific key pairs can be assigned to virtual hosts.

Auditing and Proxying Gateway Deployment

Auditing and Proxying Deployment Deployment

The following section describes the important configuration options for an auditing or proxying deployment (see Deploying for Auditing and Proxying for specific use case information).

Step	Description
Generate or Import Key Pairs and configure HTTP Listeners.	Defines the certificates and keys used to secure access to the PingAccess administrative console and secure incoming HTTPS requests at runtime.
Set up your cluster for high availability.	Facilitates high availability of critical services, and increases performance and overall system throughput.
Add trusted CA certificates.	Defines trust to certificates presented during outbound secure HTTPS connections.
Create a trusted certificate group.	Provides a trusted set of anchor certificates for use when authenticating outbound secure HTTPS connections.
Define virtual servers for protected Resources.	Allows one server to share PingAccess Resources without requiring all Sites on the server to use the same host name.